CIRCL
Computer Incident
Response Center
Luxembourg

GCVE.eu

Vulnerability Lookup and GCVE

A Decentralized Approach to Vulnerability Allocation, Publishing and Management

https://vulnerability-lookup.org – https://gcve.eu/

info@gcve.eu - @gcve@social.circl.lu

Pass The Salt - July 2, 2026

CIRCL https://www.circl.lu

Vulnerability-Lookup

Who is behind Vulnerability-Lookup?

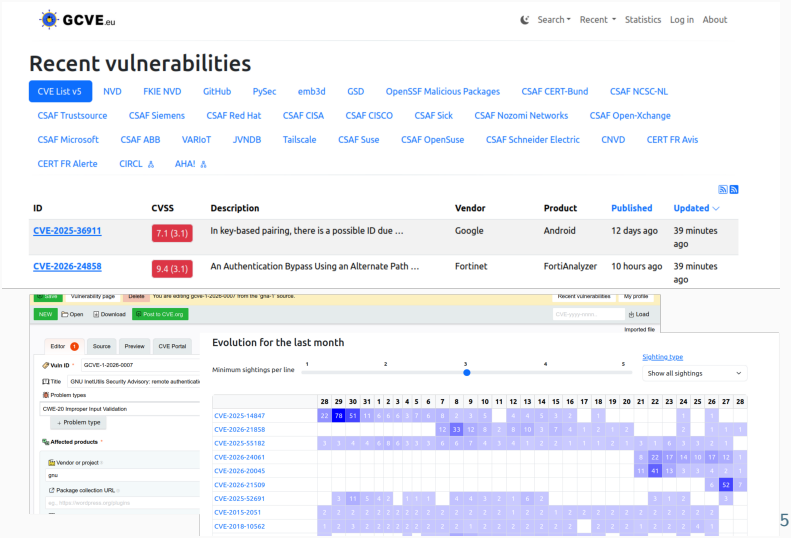
Vulnerability-Lookup[1] is an **Open Source** project led by **CIRCL**.
It is co-funded by **CIRCL** and the **European Union**[2].
Used by many organisations including CSIRTs and ENISA (EUVD).
`db.GCVE.eu` is also a vulnerability-lookup instance.

[1] `https://www.vulnerability-lookup.org`
[2] `https://github.com/ngsoti`

What is Vulnerability-Lookup?

- A unified place to **search**, **triage**, and **track** software and product vulnerabilities from different sources.
- Brings together vulnerability information, correlation of identifiers (e.g., CVE, GHSA, OSV), references, timelines, and risk signals in one view.
- Designed for **CSIRTs**, **SOCs**, **vulnerability managers**, and **developers** in mind.
- **Web UI first** with strong **API** and automation options.
- Support a complete **CVD process management**[3] along with the ability to fork vulnerability information[4]. Distributed GNA directory and GCVE/CVE automatic publication and pulling.

[3] CNA Program, GCVE GNA Publication
[4] Implemented before the GNA initiative!



[5]

[5] https://db.gcve.eu - https://vulnerability.circl.lu/

Origin of Vulnerability-Lookup

- `cve-search`[6] is an open-source tool initially developed in late 2012, focusing on maintaining a **local** CVE database.
- `cve-search` is widely used as an **internal** tool.
- The design and scalability of cve-search are limited. Our operational public instance has reached a hard limit of 20,000 queries per second.
- Vulnerability sources have **diversified**, and the **CVE is no longer the sole source** of vulnerability information.

[6] `https://github.com/cve-search/cve-search`

Developed in 2025

- **Volume of data:** Handling a substantial dataset and heavy network traffic, currently over **2,365,456** security advisories and more than **466,224** sightings collected (from MISP, Nuclei, MetaSploit, Social Networks) in approximately a year [7].
- **Flexibility:** Balancing ongoing development with legacy issues while designing a future-proof architecture. It's complex and yes, sometimes chaotic[8].
- **Robustness:** Validating data even when external entities don't comply with their own JSON schemas. It's not always pretty.
- **Fast lookup:** Rapidly correlating identifiers across **diverse sources**, including unpublished advisories.

[7] The first sighting on Exploit-DB dates back 26 years.
[8] We enjoy challenges, especially when they lead to practical solutions.

Developed in Q1-Q2 2026

- **CVD process:** Vulnerability-Lookup open source stack fully supports Coordinated Vulnerability Disclosure as CNA (CVE Program) or/and GNA (GCVE initiative). [9]
- **Vulnerability numbering:** Enabling a distributed approach via the Global CVE Allocation System. [10]
- **Scoring vulnerabilities:** Aggregating large volumes of observations from diverse advisory types to improve scoring. Automatic **weighting** of sightings by source or type (e.g., exploited, PoC available) and **detection of type** independent of the source.
- **Data quality:** Transforming messy data into clean datasets suitable for model training and analysis[11].

[9] Aligned with NIS 2 and the Cyber Resilience Act.
[10] `https://gcve.eu`
[11] https://github.com/vulnerability-lookup/VulnTrain

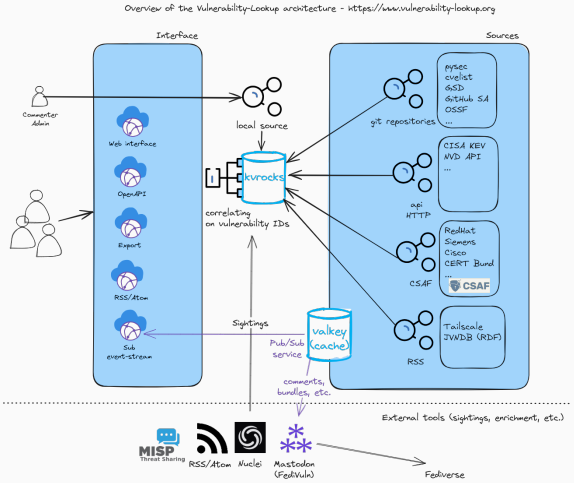
Current Sources

Source family	Feeds	Examples / coverage
Core vulnerability IDs	4	CVE List v5, NVD, FKIE NVD, Vulnrichment
Ecosystem advisories	11	GitHub Advisory DB, GSD, PySec, Bitnami, Drupal, Tailscale, OSV: AlmaLinux/Haskell/OCaml/OSS-Fuzz/RustSec
CSAF 2.0 producers	46	CERT-Bund, CISA, Cisco, Microsoft, Red Hat, SUSE/OpenSUSE, Siemens, ABB, Schneider Electric, Phoenix Contact, WAGO, SICK, Nozomi, and industrial vendors
National / sector feeds	7	CERT-FR alerts/advisories (FR), CNVD (CN), JVNDB (JP), VARIoT (PL), FSTEC (RU), Moksha (DK)
Exploitation and risk signals	5	EPSS, CISA KEV, CNW KEV, GCVE/GNA KEV feeds (GNA-1, GNA-1337)
Knowledge and supply-chain	5	CWE, CAPEC, EMB3D, CleanStart, OSSF malicious packages
Current snapshot	**78**	**2,281,288 database entries** (latest refreshes include NVD, VARIoT, Tailscale and CSAF feeds on 2026-06-10)

Feed counts are grouped from the latest collection status JSON; the CSAF row aggregates all `csaf_*` producers.

Vulnerability-Lookup High-Level Architecture

- Collects and aggregates vulnerability data.
- Preserves data integrity (**never alters the original content**).
- Harmonizes data using kvrocks.
- **Correlates** information across multiple sources (CVE, PySec, etc.).
- Provides both APIs and a Web interface.
- Supports advanced queries and filtering.



TLP:CLEAR

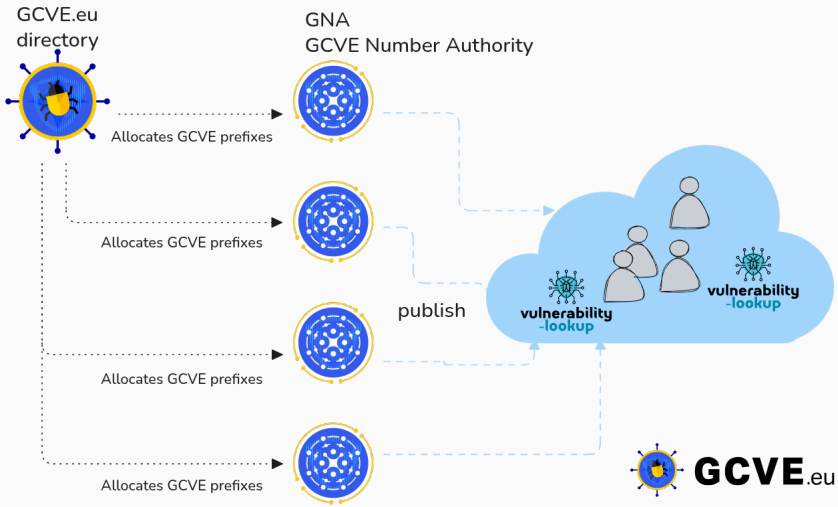
Global CVE Allocation System

Role

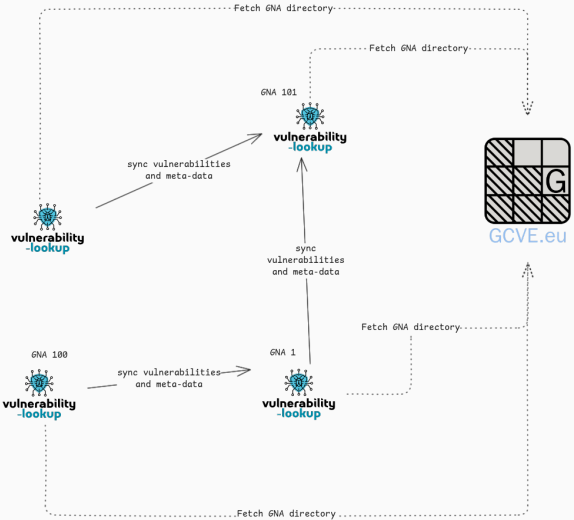
- The primary role of GCVE is to provide **globally unique identifiers** to GCVE Numbering Authorities (GNAs).
- **GNAs operate autonomously**, with full control over how they assign and manage identifiers.
- **GCVE publishes Best Current Practices (BCPs)** on directory management, Coordinated Vulnerability Disclosure (CVD), and publication protocols.
- GCVE maintains and publishes the **official directory of all GNAs**[12], including their publication endpoints.

[12] `https://gcve.eu/gna/`

Overview


GCVE.eu
directory
GNA
GCVE Number Authority
Allocates GCVE prefixes
Allocates GCVE prefixes
Allocates GCVE prefixes
Allocates GCVE prefixes
publish
vulnerability
-lookup
vulnerability
-lookup
GCVE.eu

A Distributed Network



TLP:CLEAR

Who Can Be a GNA?

- You are an existing CNA recognized by the CVE Program.
- You are not a CNA, but **meet at least one of the following conditions**[13]:
  - You are a registered CSIRT or CERT listed on FIRST.org, part of the EU CSIRTs Network, or a member of TF-CSIRT.
  - You are a software, hardware, or service provider that regularly discloses vulnerabilities affecting your own products or services, and you have an official CPE vendor[14] name assigned.
  - You have a public vulnerability disclosure policy and maintain a publicly accessible source for newly disclosed vulnerabilities in GCVE-BCP 05 format.

[13] https://gcve.eu/about/#eligibility-and-process-to-obtain-a-gna-id
[14] https://cpe.gcve.eu/

Benefits of Becoming a GNA

- **Fast, straightforward onboarding**: as soon as the eligibility criteria are met, registration is quick and simple.
- **Flexible identifier usage**: you may publish new CVE entries immediately and apply your assigned prefix to both current and historical identifiers.
- **Autonomy over publication**: each GNA determines for itself what constitutes a vulnerability and what information is made public.
- **Incremental adoption of BCPs**: additional GCVE Best Current Practices can be adopted over time; implementing every BCP is encouraged but not mandatory.

Best Current Practices (BCPs)

ID	Title	Status	Ver.	Date
GCVE-BCP-01	Signature Verification of the Directory File	**Published**	1.2	2026-03-10
GCVE-BCP-02	Practical Guide to Vulnerability Handling and Disclosure	**Published**	1.7	2026-05-02
GCVE-BCP-03	Decentralized Publication Standard	Public review	1.4	2026-03-25
GCVE-BCP-04	Recommendations and Best Practices for ID Allocation	**Published**	1.4	2026-03-10
GCVE-BCP-05	GCVE Vulnerability Format (Modified CVE Record Format)	Public review	1.7	2026-03-10
GCVE-BCP-06	Requirements and Evaluation Criteria for GCVE Numbering Authorities (GNAs)	*Draft review*	1.1	2026-03-10
GCVE-BCP-07	Known Exploited Vulnerability – KEV Assertion[15] Format	Public review	2.0	2026-03-10
GCVE-BCP-09	Scope of a GCVE Record	*Draft review*	1.0	2026-05-20
GCVE-BCP-10	Improved Common Platform Enumeration for GCVE	*Draft review*	1.0	2026-04-26

GCVE BCPs are living, community-reviewed documents. Extension: GCVE-BCP-05-X-01 defines AI-assisted vulnerability information annotation for GCVE-BCP-05.

`https://gcve.eu/bcp/`

[15] `https://gcve.eu/bcp/gcve-bcp-07/`

How to Publish with GCVE in 4 Steps

- **1.** Install `vulnerability-lookup` or generate a feed compliant with `GCVE-BCP-05`.
- **2.** Apply to become a GCVE Numbering Authority (GNA) and submit your feed URL.
- **3.** Your feed is now discoverable and consumable by all software in the GCVE network.
- **4.** Make some tea.

cpe.gcve.eu - Fixing the Mess of Vendor/Product cataloguing

A collaborative catalog for vulnerability metadata

- New GCVE service[16] dedicated to **vendor, product, CPE URI and PURL curation**.
- Provides a focused workspace for maintainers, reviewers and consumers of security metadata.
- Goal: improve the quality of platform naming used in vulnerability management workflows.

Why this matters

- CPEs are central to identifying affected software, hardware and operating systems.
- PURL support enables better pivots between package ecosystems and product records.
- Better naming improves matching, enrichment and downstream vulnerability intelligence.

[16] https://cpe.gcve.eu/

cpe.gcve.eu: service workflow

From discovery to distribution

Discover	Search canonical platform names across vendor, product, CPE URI and PURL fields.
Propose	Submit improvements, additions or corrections through a proposal workflow.
Moderate	Review proposals and notes before accepting changes into the catalog.
Distribute	Expose approved changes through history, API access and dataset export.

`https://cpe.gcve.eu/`

cpe.gcve.eu: role in the GCVE ecosystem

Service value

- Complements **db.gcve.eu** by improving product and platform metadata.
- Supports transparent, community-driven correction of CPE/PURL mappings.
- Creates a reusable reference catalog for vulnerability lookup and enrichment.

Practical use cases

- Vendors and GNAs can align product names and identifiers.
- Analysts can pivot from package coordinates to vendor/product records.
- Tooling can consume the API/export instead of maintaining private mappings.

GCVE enriched dumps & AI extension

New service outcome

- Publishes **GCVE enriched dumps**[17]: original vulnerability records plus machine-generated severity metadata.
- Current enrichment uses **VLAI**[18], a RoBERTa-based severity classifier, inferred from vulnerability descriptions.
- Enrichment is stored as GCVE extensions, without replacing the original record.

Key value

- **Traceable**: uses BCP-05-X-01 AI provenance annotations.
- **Reproducible**: tooling available for single records and full dumps.
- **Operational**: adds a non-authoritative triage signal for large-scale processing.

[17] https://github.com/gcve-eu/gcve-enriched-dumps
[18] https://www.vulnerability-lookup.org/user-manual/ai/

Roadmap

- Vulnerability-Lookup version 5.3 (end of July): multi-user and multi-organisation publication workflow.
- GCVE record format extensions (by end of 2026), with CVE record format compatibility, including ADP(?) and **extension support**.
- CRA-oriented **SBOM handling** and checking in Vulnerability-Lookup (by end of 2026).
- Self-reference vulnerability via commit-id as GCVE identifier.
- GCVE GNA to create "flash-vulnerability" disclosure.
- Any ideas? join us.

References

https://www.vulnerability-lookup.org - https://gcve.eu/

https://vulnerability.circl.lu - https://db.gcve.eu/ - https://cpe.gcve.eu/

https://github.com/vulnerability-lookup/vulnerability-lookup

https://social.circl.lu/@gcve

Thank you for your attention

- Issues, new sources of advisories or ideas:
  `https://github.com/vulnerability-lookup/vulnerability-lookup`
- For support and questions, contact: info@circl.lu
- If you want to become a GNA, gna@gcve.eu
- GCVE **@@gvce@social.circl.lu**